

AFFIDAVIT
of
TRACY PERKINS
DETECTIVE
BOONE COUNTY SHERIFF'S OFFICE

I, Tracy Perkins, being first duly sworn, do depose and state that:

1. I am a federally deputized Detective, with the Boone County Sheriff's Office, and am assigned to the Cyber Crimes Task Force in Columbia, Missouri. Over my 28-year career, I have over 2000 hours of certified law enforcement training. I was assigned to the Task Force in 2007 and hold several hundred hours in the investigation and exploitation of children through the Internet. I have participated in numerous investigations concerning violations of Title 18, United States Code. I have gained expertise in the conduct of such investigations through training in seminars, trainings, and everyday work related to these types of investigations. I have personally led multiple investigations involving the exploitation of children.

2. As a State law enforcement officer, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. At all times throughout this affidavit I use the term "child pornography" merely as shorthand to refer to visual depictions of actual minors engaged in sexually explicit conduct. I use the terms "visual depiction," "minor" and "sexually explicit conduct" as those terms are defined in 18 U.S.C. § 2256 (see below).

3. I am investigating activities occurring on the electrical devices described in Attachment A ("the Devices") seized from Luis Alberto Narvaez-Fonseca on September 9, 2021. As will be shown below, there is probable cause to believe NARVAREZ-FONSECA used the Devices to facilitate the sexual exploitation of children, including the receipt/distribution and/or possession of child pornography, all in violation of Title 18, United States Code, Section 2252. I

am submitting this affidavit in support of a search warrant authorizing a search of the Devices, which items constitute instrumentalities, fruits and evidence of the foregoing violations. I am requesting authority to search the electrical devices described in Attachment A for the items specified in Attachment B, and to seize all items listed in Attachment B as instrumentalities, fruits and evidence of crime.

4. The statements contained in this affidavit are based on information I learned through my personal knowledge, and interview of NARVAREZ-FONSECA. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B), specifically receipt/distribution and possession of child pornography, are located within the Devices seized from Narvaez-Fonseca on September 9, 2021.

Statutory Authority

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors. Title 18, United States Code, Section 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce. Title 18, United States Code, Section 2252A prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child

pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

Definitions

6. The following definitions apply to this Affidavit and Attachments A & B:
 - a. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions;
 - b. “Child Pornography,” as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (See 18 U.S.C. §§ 2252 and 2256(2));
 - c. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5);
 - d. “Minor,” as used herein, means any person under the age of eighteen (18) years;
 - e. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2);
 - f. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device”;
 - g. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit

electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks);

h. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications and utilities;

i. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items;

j. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it;

k. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet; and

l. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives,

or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

7. Based on my training and experience, I know images of child pornography and communications regarding the sexual exploitation of children, including the receipt/distribution and/or possession of child pornography, can be stored on computer hardware. Based on my training and experience, examining data stored on these types of devices can uncover, among other things, evidence that reveals or suggests who possessed or used the Device(s), as well as evidence of participation in and commission of the crimes being investigated.

Background of the Investigation

8. On January 25, 2021, March 3, 2021 and September 1, 2021, the Boone County Sheriff's Office Cyber Crimes Task Force received multiple CyberTip reports from the National Center for Missing and Exploited Children, known as NCMEC. The National Center for Missing and Exploited Children operates a web-based reporting system that facilitates the reporting of Internet related crimes against children. NCMEC received information from Google reference the upload of over 3000 suspected child pornography files. I have reviewed a sample of the files. The content contained both images and videos depicting young prepubescent females between 4 to 12 years old engaging in sexual conduct with adult males, and other children or the children displaying their genitals in sexually explicit conduct.

9. The NCMEC reports showed the account holder as "Luis Alberto Narvaez Fonseca", date of birth 10-21-1970 with mobile 573-353-7368 and email address "langperlita@gmail.com" (verified). I checked Missouri Department of Revenue and found the subject resides in Jefferson City, Missouri. Furthermore, records were obtained on the cell phone number and the address listed was the same location where NARVAEZ-FONSECA lived in Jefferson City, Missouri.

10. On September 8, 2021, I requested the Cole County Sheriff's Office attempt to locate NARVAEZ-FONSECA on two outstanding warrants. On said day, the Cole County Sheriff's Office advised they had arrested NARVAEZ-FONSECA. In addition, the Cole County detectives advised they had seized a cell phone from his person. The following day, I interviewed NARVAEZ-FONSECA at the Cole County Sheriff's Office interview room. Post Miranda, NARVAEZ-FONSECA identified the phone number and ownership of email addresses associated with two separate Google accounts langperlita@gmail.com and perlitalanf@gmail.com. During the interview, NARVAEZ-FONSECA further acknowledged that he knew CSAM files were associated with his Google accounts and several child pornography files were going to be located on his Samsung S9+ cellular phone. The defendant provided a password for this device. The Device was seized for examination.

11. During the interview I was granted written permission from NARVAEZ-FONSECA to search his bedroom located at 3005 Southwood Hills, in Jefferson City, Missouri.

12. On September 10, 2021, Task Force Detective Cody Bounds and I contacted NARVAEZ-FONSECA mother, Auxiliadora "Alex" Amundson at this address. I spoke with Alex about the ongoing investigation and charges against her son. I advised Alex her son, NARVAEZ-FONSECA had given me written permission to search his bedroom and showed her a copy of the authorization. Alex agreed for us to search NARVAEZ-FONSECA bedroom. During the search, Detective Bounds located a Samsung III cellular phone under the bed. This Device was seized for examination.

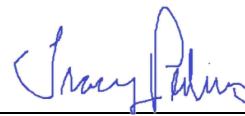
Conclusion

13. Based upon the foregoing, I assert that probable cause exists the Devices seized from Luis Alberto Narvarez-Fonseca on September 9, 2021, contains evidence of the sexual exploitation

of children, including the receipt/distribution and/or possession of child pornography, all in violation of Title 18, United States Code, Sections 2252(a)(2) and 2252(a)(4)(B) and the Device seized on September 10, 2021 contains possible evidence of child pornography directly linked to Narvarez-Fonseca.

14. The facts set forth in this affidavit are true and correct to the best of my knowledge and belief.

FURTHER, AFFIANT SAYETH NOT.



Tracy Perkins, Detective
Boone County Sheriff's Office

Sworn and subscribed to me by telephone on this 1st day of December 2021.



HONORABLE WILLIE J. EPPS, JR.
United States Magistrate Judge
Western District of Missouri